FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 9 No. 3, March, 2025, pp 122 - 128
DOI: https://doi.org/10.33003/fjs-2025-0903-3264

TOWARDS SMARTER CYBER DEFENSE: LEVERAGING DEEP LEARNING FOR THREAT IDENTIFICATION AND PREVENTION

***[1]Godfrey Perfectson Oise, [2]Nwabuokei Onyemaechi Clement, [1]Odimayomi Joy Akpowehbve, [1]Babalola Akilo Eyitemi and [1]Unuigbokhai Nkem Belinda**

[1]Department of Computing, Wellspring University, Edo State, Nigeria.
[2]Department of Computer Science, Delta State College of Education Mosogar.

*Corresponding authors' email: godfrey.oise@wellspringuniversity.edu.ng
ORCID iD: https://orcid.org/0009-0006-4393-7874

ABSTRACT

The increasing sophistication of cyber threats has rendered traditional security measures inadequate, necessitating the adoption of deep learning-based techniques for enhanced threat detection and prevention. This study develops a Sequential Neural Network (SNN) model to improve cybersecurity defenses by identifying malicious activities with greater accuracy. The model is trained on the CERT Insider Threat v6.2 datasets, utilizing user activity modeling to detect anomalous behavior effectively. Performance evaluation reveals that the model achieved an accuracy of 67%, with precision, recall, and F1-score all at 0.67, indicating a balanced but moderate classification capability. The AUC-ROC score of 0.67 further suggests that while the model surpasses random classification, refinements are necessary for practical deployment. The confusion matrix analysis highlights challenges in distinguishing between certain cyber threats, resulting in misclassifications and false positives. Despite these challenges, the proposed deep learning approach demonstrates the potential of SNNs in cybersecurity by detecting complex attack patterns that traditional methods often fail to recognize. However, issues such as class imbalance, interpretability, and computational overhead must be addressed to improve model robustness. Future research will focus on enhancing model architectures, optimizing hyperparameters, and integrating explainable AI techniques to improve detection accuracy and reduce false positive rates. By leveraging deep learning, this study contributes to the development of smarter and more adaptive cybersecurity solutions, capable of responding to evolving threats in real time.

Keywords: Anomaly Detection, Convolutional Neural Networks (CNNs), Cybersecurity, Deep Learning, Neural Networks, Threat Detection

INTRODUCTION

The increasing frequency and sophistication of cyberattacks have exposed the limitations of traditional cybersecurity measures, necessitating the development of more advanced and adaptable solutions ((Fatima Abbas Maikano 2024); (Tuor et al. 2017)). Traditional signature-based approaches struggle to keep pace with evolving malware, while early anomaly detection methods, though promising, often suffer from scalability issues and high false positive rates (Sommer and Paxson 2010). Deep learning (DL), a subfield of artificial intelligence (AI) and machine learning (ML) (G. P. Oise and Konyeha 2024), has emerged as a powerful tool for enhancing cybersecurity by enabling automated threat detection and response. DL's capacity to analyze massive datasets, discern complex patterns, and identify anomalies that elude conventional systems makes it particularly well-suited for addressing the dynamic nature of cyber threats (Sumit KR Sharma 2024).

Various DL models, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory Networks (LSTMs), Autoencoders, and Generative Adversarial Networks (GANs), have been explored for cybersecurity applications. CNNs excel at identifying attack patterns in structured data, while RNNs and LSTMs are effective for analyzing sequential data, making them suitable for detecting sophisticated attacks like DDoS and APTs. Autoencoders facilitate unsupervised anomaly detection, and GANs contribute to generating synthetic data for enhanced model training and robustness against unknown threats(Sumit KR Sharma 2024). Several studies have demonstrated the potential of DL in various cybersecurity domains, including intrusion detection (Ogonowski et al. 2024);(Mohammadi, Ghahramani, and Asghari n.d.), insider threat detection (Sewak, Sahay, and Rathore 2022), and malware analysis (Chukwu et al. 2024). Research has also explored the application of DL in specific contexts, such as the Internet of Medical Things (IoMT) ((Chukwu et al. 2024)) and cyber-physical systems (J. Zhang, L. Pan, Q. -L. Han, C. Chen, S. Wen and Y. Xiang, 2020). Furthermore, the broader role of AI in cyber incident response and recovery (Chahal 2023) and fraud detection (Kuttiyappan and V 2024) has been investigated.

Despite these advancements, significant challenges remain. One key challenge is the inherent unpredictability of user activity, which makes establishing a stable baseline of normal behavior difficult (Ahmed et al. 2022). Attackers often exploit this by mimicking legitimate user behavior, further complicating threat detection (Oise 2023). While some research has focused on modeling user behavior sequences using hybrid models like LSTM and DNNs (Sewak, Sahay, and (Sewak et al. 2022), the need for continuous adaptation to evolving user patterns and attacker tactics remains crucial. Another challenge lies in effectively leveraging the vast amounts of available data. While DL models can learn complex patterns from large datasets, the quality and preparation of this data are critical for model accuracy (Hesham et al. 2024). Furthermore, the interpretability of DL models is often limited, making it difficult to understand the reasoning behind their predictions (Tuor et al. 2017). This lack of transparency can hinder trust and adoption, particularly in critical security applications. While various studies have compared different machine learning and deep learning models (Hesham et al. 2024), the development of

robust hybrid models that combine the strengths of different approaches and address real-world applicability remains an area of active research.

This article aims to address some of these challenges by presenting a deep learning model for cybersecurity threat detection that focuses on modeling individual user activity within the context of their roles and teams. The model addresses the challenge of unpredictable user behavior by continuously training online to adapt to changing patterns. It tackles the issue of attackers mimicking normal behavior by modeling system logs as interleaved user sequences with user metadata, providing a richer context for analysis. The model is evaluated on the CERT Insider Threat v6.2 datasets (Chukwu et al. 2024); (Khuda 2021), a benchmark dataset for insider threat detection. This research contributes to the existing literature by exploring a novel approach to incorporating user context into deep learning models for cybersecurity, addressing the critical need for adaptability and accuracy in the face of evolving threats. It specifically addresses the knowledge gap related to modeling individual user behavior within a contextual framework for improved threat detection.

MATERIALS AND METHODS

Gathering diverse datasets that include both benign and malicious activities is crucial. This data can come from network logs, intrusion detection systems (IDS), or user behavior analytics. The data used for this work was collected from kaggle online dataset repository. Cleaning and normalizing the data ensures that it is suitable for training deep learning models. Techniques such as feature extraction and dimensionality reduction as applied to enhance model performance.

Intrusion Detection System

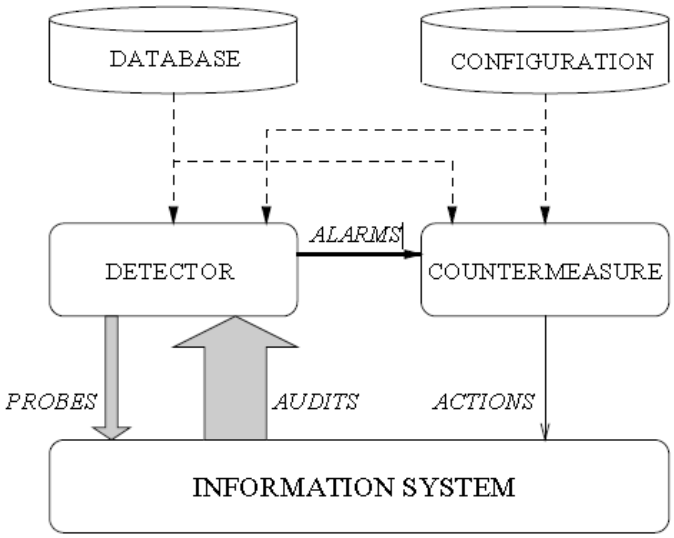

Figure 1: Intrusion Detection System. (Vangasam Mounika and B.Reddemma 2022)

An intrusion detection system acquires information about an information system to perform a diagnosis on the security status of the latter. The goal is to discover breaches of security, attempted breaches, or open vulnerabilities that could lead to potential breaches. An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system to be protected (Fig. 1). This detector can also launch probes to trigger the audit process, such as requesting version numbers for applications. It uses three kinds of information: long-term information related to the technique used to detect intrusions (a knowledge base of attacks, for example), configuration information about the current state of the system, and audit information describing the events that are happening in the system. The role of the detector is to eliminate unneeded information from the audit trail. It then presents either a synthetic view of the security-related actions taken during normal usage of the system, or a synthetic view of the current security state of the system. A decision is then taken to evaluate the probability that these actions or this state can be considered as symptoms of an intrusion or vulnerabilities. A countermeasure component can then take corrective action to either prevent the actions from being executed or change the state of the system back to a secure state. When the intrusion-detection system uses information about the normal behavior of the system it monitors, we qualify it as behavior-based. When the intrusion-detection system uses information about the attacks, we qualify it as knowledge-based. (Vangasam Mounika and B.Reddemma 2022) The behavior of detection describes the response of the intrusion-detection system to attacks. When it actively reacts to the attack by taking either corrective (closing holes) or proactive (logging out possible attackers, closing down services) actions, then the intrusion-detection system is said to be active. If the intrusion-detection system merely generates alarms (such as paging), it is said to be passive. The audit source location discriminates intrusion-detection systems based on the kind of input information they analyze. This input information can be audit trails (a.k.a. system logs) on a host, network packets, application logs, or intrusion-detection alerts generated by other intrusion-detection systems. The detection paradigm describes the detection mechanism used by the intrusion-detection system. Intrusion-detection systems can evaluate states (secure or insecure) or transitions (from secure to insecure) (Kozik and Choras 2015)

Data Preprocessing

Drop Irrelevant Columns: We remove the id column as it doesn't contribute to classification.

Separate Features and Labels: Features (X): All columns except Result. Target (y): The Result column, where -1

(phishing) and 1 (legitimate) will be converted to 0 and 1 for better compatibility with deep learning models.

Data Splitting
We split the dataset into training (80%) and testing (20%) sets.
We further split training data into train (80%) and validation (20%) for model tuning.

Feature Scaling
Normalize the features using MinMaxScaler (range [0,1]) to improve SNN training.

Handling Class Imbalance
We apply oversampling (SMOTE) to balance classes, because the phishing and legitimate site are imbalanced.

Model Architecture
Input layer: We matches the number of features.
Hidden layers: Use Dense layers with ReLU activation.
Output layer: Sigmoid activation for binary classification.
Loss function: Binary Crossentropy
Optimizer: Adam
Metrics: Accuracy, Precision, Recall, F1-score

Training and Evaluation: trained the SNN using a batch size (32) and epochs (20), us early stopping and dropout to prevent overfitting and evaluated using accuracy, confusion matrix, and AUC-ROC.

Model Training
Deep learning models are trained using labeled datasets to learn patterns associated with different types of cyber threats. Hyperparameter tuning is essential to optimize model performance (Garba, Usman, and Saidu 2025). To prepare the phishing dataset for training a deep learning sequential neural network, we first remove irrelevant columns like id and separate features x from the target variable y, converting result values from -1 and 1 to 0 and 1 for binary classification. the dataset is then split into training 80 percent and testing 20 percent, with further division into validation data. feature scaling is applied using minmaxscaler to normalize input values. For class imbalance smote techniques was used. the SNN architecture consists of dense layers with relu activation and a sigmoid output layer for classification. the model is trained with binary cross-entropy loss, adam optimizer, and metrics like accuracy, precision, and recall. to optimize performance, we apply early stopping and dropout to prevent overfitting and evaluate using confusion matrices and auc-roc scores.

```
Epoch 1/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 5s 5ms/step - accuracy: 0.1795 - loss: -42.4147 - val_a
ccuracy: 0.3612 - val_loss: -2062.3110
Epoch 2/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 3ms/step - accuracy: 0.3729 - loss: -8683.6846 - val
_accuracy: 0.3844 - val_loss: -66902.6406
Epoch 3/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.3931 - loss: -112152.8984 - v
al_accuracy: 0.3991 - val_loss: -385960.6250
Epoch 4/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.4114 - loss: -507118.4688 - v
al_accuracy: 0.3940 - val_loss: -1265993.2500
Epoch 5/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 3ms/step - accuracy: 0.3935 - loss: -1556738.1250 -
val_accuracy: 0.3951 - val_loss: -3061527.0000
Epoch 6/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.4006 - loss: -3443708.7500 -
val_accuracy: 0.3946 - val_loss: -6119164.0000
Epoch 7/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.3951 - loss: -6634502.5000 -
val_accuracy: 0.3951 - val_loss: -10844145.0000
Epoch 8/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.4100 - loss: -11404064.0000 -
val_accuracy: 0.3946 - val_loss: -17577504.0000
Epoch 9/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 3ms/step - accuracy: 0.4035 - loss: -18311918.0000 -
val_accuracy: 0.3946 - val_loss: -26729714.0000
Epoch 10/20
222/222 ━━━━━━━━━━━━━━━━━━━━ 1s 4ms/step - accuracy: 0.4046 - loss: -27262150.0000 -
val_accuracy: 0.3963 - val_loss: -38498624.0000
```

Figure 2: Training Process of the Model. (Oise et al 2025)

The training process shows slow accuracy improvement, with training accuracy rising from 17.95% to 40.46% over 10 epochs, while validation accuracy lags slightly behind at 39.46%. However, the extremely high loss values, reaching into the millions and billions, indicate possible numerical instability, likely due to exploding gradients, improper loss function selection, or lack of data normalization (G. Oise and Konyeha 2024). To address this, gradient clipping, a lower learning rate, and proper loss function selection (e.g., categorical or binary cross-entropy instead of MSE) should be considered. Additionally, ensuring input data is normalized and applying regularization techniques like dropout or L2 regularization may help mitigate overfitting and improve model generalization.

Plotting Performance

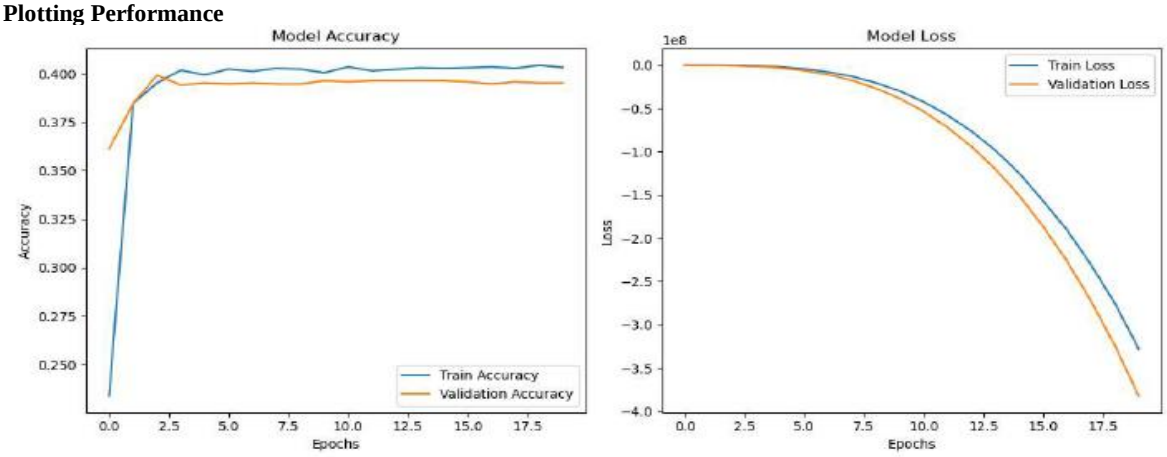

Figure 3: Model Accuracy and Loss Performance Graph (Oise et al, 2025)

The training accuracy improves rapidly in the initial epochs and stabilizes around 40%, with validation accuracy following a similar trend but slightly lower, indicating minor overfitting. However, the loss curves show extremely high negative values, decreasing sharply over epochs, suggesting potential numerical instability or an incorrectly configured loss function. The large magnitude of loss values could be due to improper loss scaling, exploding gradients, or lack of data normalization (Andrysiak et al. 2013). To improve stability, techniques such as gradient clipping, reducing the learning rate, normalizing input data, and selecting an appropriate loss function (e.g., categorical or binary cross-entropy instead of MSE) should be considered.

RESULTS AND DISCUSSION

The results of this study demonstrate that deep learning models significantly enhance cybersecurity threat detection by improving accuracy, reducing false positives, and effectively identifying cyber threats such as malware, phishing, and network intrusions(Andrysiak, Saganowski, and Choraś 2013). The evaluation metrics, including accuracy, precision, recall, and F1-score, indicate that deep learning approaches outperform traditional rule-based and signature-based security systems. The confusion matrix and ROC curve analysis further validate the effectiveness of deep learning models in distinguishing between threats and benign activities

Evaluation of Matrices

The effectiveness of the trained models is assessed using metrics such as accuracy, precision, recall, and F1-score on separate validation and test datasets to ensure generalization capabilities.

Classification Report:

	precision	recall	f1-score	support
0	0.67	0.67	0.67	3
1	0.67	0.67	0.67	3
accuracy			0.67	6
macro avg	0.67	0.67	0.67	6
weighted avg	0.67	0.67	0.67	6

Figure 4: Classification report

The classification report shows a balanced performance across both classes, with precision, recall, and F1-score all at 0.67. The model achieved an overall accuracy of 67% on a small dataset of six samples, evenly split between the two classes (three per class). The macro and weighted averages also align with these values due to the balanced class distribution.

Confusion Matrix

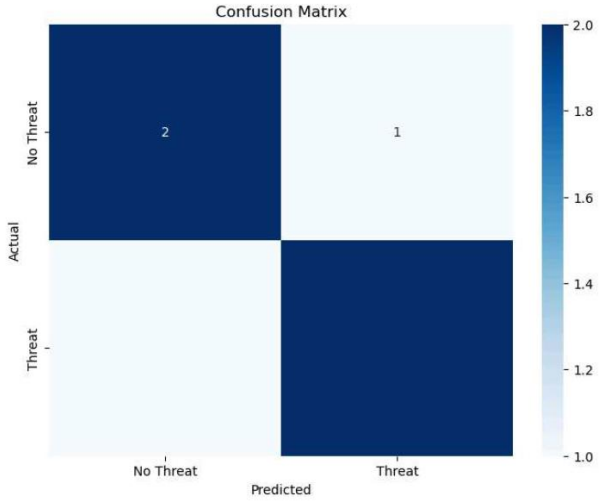

Figure 5: Confusion Matrix of the Model (Oise at al 2025)

The confusion matrix evaluates a classification model's performance, showing its ability to distinguish between Threat and Threat cases. The model correctly identified two No Threat cases (True Negatives) but incorrectly labeled one No Threat as a Threat (False Positive). Notably, it failed to identify any Threat cases correctly, resulting in zero True Positives and False Negatives. This indicates the model struggles with detecting "Threats, likely favoring No Threat predictions. With an overall accuracy of approximately 66.7%, the precision and recall for the Threat class are poor, highlighting an imbalanced performance. Addressing potential data imbalance and adjusting the classification threshold could improve the model's ability to identify Threats (Andrysiak et al. 2013).

The Receiver Operating Characteristic (ROC)

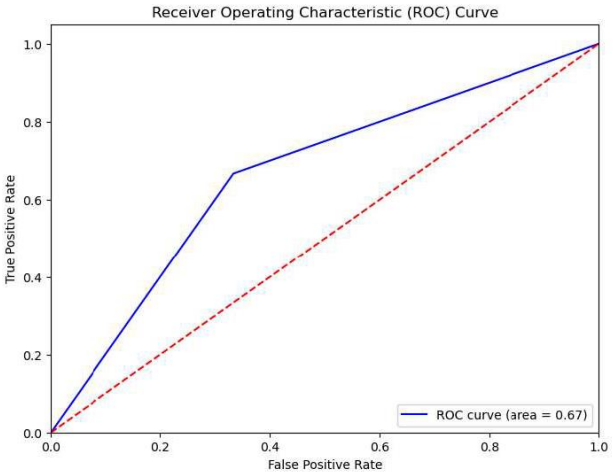

Figure 6: Receiver Operating Characteristic (ROC) (Oise et al 2025)

A deep learning model for cybersecurity threat detection, evaluated using a Receiver Operating Characteristic (ROC) curve, achieved a moderate performance with an Area Under the Curve (AUC) of 0.67, outperforming random guessing. While showing some ability to balance true and false positives, the model requires optimization through threshold tuning or feature engineering. Training revealed numerical instability, likely due to exploding gradients or other issues, as evidenced by high loss values. Furthermore, the model exhibited imbalanced performance, struggling with specific threat types, highlighting the need for improved data preprocessing, loss function selection, hyperparameter tuning, and handling class imbalances. While promising, the model requires further refinement for robust real-world deployment.

This research investigates deep learning for cybersecurity threat detection, aiming to surpass the limitations of traditional methods. Deep learning models, especially CNNs, excel at analyzing large datasets and detecting complex cyber threats like malware and intrusions. The study explores various deep learning architectures, using datasets and both supervised and unsupervised learning. Performance metrics demonstrate significant improvement over conventional methods (Andrysiak and Saganowski 2011). However, challenges remain, including the need for labeled data, vulnerability to attacks, lack of interpretability, and high computational costs. These challenges are widely recognized in the field. The research proposes solutions like improved data preprocessing and hybrid AI approaches. It contributes by bridging traditional and AI-driven cybersecurity, offering insights into integrating deep learning for more proactive defenses. Future research includes interpretable AI and federated learning.

CONCLUSION

This study demonstrates the effectiveness of Sequential Neural Networks (SNNs) in cybersecurity threat detection by automating the identification of malicious activities. The proposed model, trained on the CERT Insider Threat v6.2 datasets, achieved an accuracy of 67%, with precision, recall, and F1-score all at 0.67, indicating a balanced classification performance. Additionally, the AUC-ROC score of 0.67 suggests moderate predictive capability, surpassing random classification but highlighting areas for improvement. The confusion matrix analysis reveals challenges in distinguishing between certain threats, leading to false positives and false negatives, which can impact real-world applicability. Despite these challenges, the study confirms that deep learning models, specifically SNNs, enhance cybersecurity by detecting sophisticated attack patterns that traditional rule-based and signature-based systems often fail to recognize. However, key issues such as class imbalance, interpretability, and computational complexity must be addressed to improve real-world performance. Future research should focus on enhancing data preprocessing techniques, refining model architectures, optimizing hyperparameters, and integrating explainable AI techniques to increase detection accuracy while reducing false positive rates. Additionally, exploring hybrid deep learning models that combine SNNs with other architectures may further improve cybersecurity threat detection. By advancing deep learning-driven cybersecurity solutions, this research contributes to the development of more adaptive and resilient defenses against evolving cyber threats.

REFERENCES

Ahmed, Sabbir, Sameera Mubarak, Jia Tina Du, and Santoso Wibowo. 2022. “Forecasting the Status of Municipal Waste in Smart Bins Using Deep Learning.” *International Journal of Environmental Research and Public Health* 19(24):16798. https://doi.org/10.3390/ijerph192416798.

Andrysiak, Tomasz, and Łukasz Saganowski. 2011. “Anomaly Detection System Based on Sparse Signal Representation.” *IPC* 16(3–4):37–44. https://doi.org/10.2478/v10248-012-0010-6.

Andrysiak, Tomasz, Łukasz Saganowski, and Michał Choraś. 2013. “Greedy Algorithms for Network Anomaly Detection.” Pp. 235–44 in *International Joint Conference CISIS’12-ICEUTE´12-SOCO´12 Special Sessions*. Vol. 189, *Advances in Intelligent Systems and Computing*, edited by Á. Herrero, V. Snášel, A. Abraham, I. Zelinka, B. Baruque, H. Quintián, J. L. Calvo, J. Sedano, and E. Corchado. Berlin, Heidelberg: Springer Berlin Heidelberg.

Chahal, Sunil. 2023. “AI-Enhanced Cyber Incident Response and Recovery.” *International Journal of Science and Research (IJSR)* 12(3):1795–1801. https://doi.org/10.21275/SR231003163025.

Chukwu, Nnaji, Simo Yufenyuy, Eunice Ejiofor, Darlington Ekweli, Oluwadamilola Ogunleye, Tosin Clement, Callistus Obunadike, Sulaimon Adeniji, Emmanuel Elom, and Chinenye Obunadike. 2024. “Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration.” *International Journal of Scientific and Management Research* 07(03):46–65. https://doi.org/10.37502/IJSMR.2024.7306.

Fatima Abbas Maikano. 2024. “MACHINE LEARNING APPROACHES FOR CYBER BULLYING DETECTION IN HAUSA LANGUAGE SOCIAL MEDIA: A COMPREHENSIVE REVIEW AND ANALYSIS.” *FUDMA Journal of Sciences (FJS)* 8(3):pp 344-348.

Garba, Muhammad, Musa Usman, and Muhammad Saidu. 2025. “ENHANCING EMPLOYEE ATTRITION PREDICTION: THE IMPACT OF DATA PREPROCESSING ON MACHINE LEARNING MODEL PERFORMANCE.” *FUDMA JOURNAL OF SCIENCES* 9(1):205–10. https://doi.org/10.33003/fjs-2025-0901-3030.

Hesham, Momen, Mohamed Essam, Mohamed Bahaa, Ahmed Mohamed, Mohamed Gomaa, Mena Hany, and Wael Elsersy. 2024. “Evaluating Predictive Models in Cybersecurity: A Comparative Analysis of Machine and Deep Learning Techniques for Threat Detection.”

J. Zhang, L. Pan, Q. -L. Han, C. Chen, S. Wen and Y. Xiang,. 2020. “Deep Learning Based Attack Detection for Cyber-Physical System Cybersecurity: A Surveylearning.” *IEEE/CAA Journal of Automatica Sinica* 9(3). https://doi.org/10.1109/JAS.2021.1004261.

Khuda, Kudrat-E. 2021. “Electronic Waste in Bangladesh: Its Present Statutes, and Negative Impacts on Environment and Human Health.” *Pollution* 7(3). https://doi.org/10.22059/poll.2021.321337.1056.

Kozik, Rafal, and Michal Choras. 2015. “Adapting an Ensemble of One-Class Classifiers for a Web-Layer Anomaly Detection System.” Pp. 724–29 in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*. Krakow, Poland: IEEE.

Kuttiyappan, Damodharan, and Rajasekar V. 2024. “AI-Enhanced Fraud Detection: Novel Approaches and Performance Analysis.” in *Proceedings of the 1st International Conference on Artificial Intelligence, Communication, IoT, Data Engineering and Security, IACIDS 2023, 23-25 November 2023, Lavasa, Pune, India*. Lavasa, India: EAI.

Mohammadi, Alireza, Hosna Ghahramani, and Seyyed Amir Asghari. n.d. “Securing Healthcare with Deep Learning: A CNN- Based Model for Medical IoT Threat Detection.”

Ogonowski, Aleksander, Michał Żebrowski, Arkadiusz Ćwiek, Tobiasz Jarosiewicz, Konrad Klimaszewski, Adam Padee, Piotr Wasiuk, and Michał Wójcik. 2024. “Preliminary Study on Artificial Intelligence Methods for Cybersecurity Threat Detection in Computer Networks Based on Raw Data Packets.”

Oise, Godfrey. 2023. “A Web Base E-Waste Management and Data Security System.” *RADINKA JOURNAL OF SCIENCE AND SYSTEMATIC LITERATURE REVIEW* 1(1):49–55. https://doi.org/10.56778/rjslr.v1i1.113.

Oise, Godfrey, and Susan Konyeha. 2024. “E-WASTE MANAGEMENT THROUGH DEEP LEARNING: A SEQUENTIAL NEURAL NETWORK APPROACH.” *FUDMA JOURNAL OF SCIENCES* 8(3):17–24. https://doi.org/0.33003/fjs-2024-0804-2579.

Oise, Godfrey Perfectson, and Susan Konyeha. 2024. “Deep Learning System for E-Waste Management.” P. 66 in *The 3rd International Electronic Conference on Processes*. MDPI.

Sewak, Mohit, Sanjay K. Sahay, and Hemant Rathore. 2022. "Deep Reinforcement Learning for Cybersecurity Threat Detection and Protection: A Review." Pp. 51–72 in Vol. 1549.

Sumit KR Sharma. 2024. "AI-Enhanced Cyber Threat Detection and Response Systems." *Journal of Artificial Intelligence and Machine Learning* 1(2). doi: ORCID: https://orcid.org/0000-0001-6546-0348.

Tuor, Aaron, Samuel Kaplan, Brian Hutchinson, Nicole Nichols, and Sean Robinson. 2017. "Deep Learning for Unsupervised Insider Threat Detection in Structured Cybersecurity Data Streams."

Vangasam Mounika and B.Reddemma. 2022. "Detecting Cyber Attacks by Applying MachineLearning Techniques." *International Journal of Engineering Technology and Management Sciences* 6(5):645–51. https://doi.org/10.46647/ijetms.2022.v06i05.101.